

# THE FUTURE OF ALT DATA: IMPACT OF CCPA AND INCREASING REGULATORY SCRUTINY

May 8, 2020  
11:30 am – 12:30 pm

---

**Andrea Arias**  
Attorney  
Federal Trade  
Commission

**Stacey  
Brandenburg**  
Shareholder  
ZwillGen

**Matthew Senatore**  
COO & General  
Counsel  
Earnest Research

The views expressed are those of the speaker and not necessarily those of the FTC, any one of its Commissioners, Earnest Research, or ZwillGen PLLC.

# Agenda

- Introductions
- Framework for Alternative Data
- Discussion of Consumer Data
  - Regulator's View
  - Impact of CCPA
  - Industry's Approach to Diligence and Other Considerations
- Considerations for Use of Data
- New Challenges

# Framework for Alternative Data

- **Consumer Data:** Data obtained allegedly through consent of users (app data, credit card/financial transaction data, survey data, email receipt data)
- **Exhaust Data:** Data that a business generates or has in the ordinary course
- **Public Spaces:** Data obtained allegedly from public spaces (satellite insights data, drone data, surveillance footage, dropcam data)
- **Web scraping:** Data obtained from Internet sources without express consent of source (web scraping, APIs)

# Consumer Data

- Legal threshold – Is there legally sufficient consent to collect, share, and use the data from the consumer?
  - Fact-specific analysis
  - For geolocation data or data collection practices that consumers would not reasonably expect, may also want just-in-time or more robust notice.
- FTC, State AGs, and other regulators have views on consent:
  - LA City Attorney sued The Weather Channel App for failing to disclose sharing of location information with third parties.
  - Privacy policy contained disclosure, but alleged deception/material omission by omitting that disclosure from pop-up.

# FTC Cases – Unrollme

- Unrollme, Inc. is an email management company that helps users unsubscribe from unwanted email subscriptions.
- Unrollme got access to consumers' email accounts and shared users' email receipts with Unrollme's parent company for market research analytics.
- Prohibited from future misrepresentations.
- Must notify consumers.
- Must also delete the stored e-receipts it had already collected, unless consumers provided affirmative express consent for Unrollme to keep the e-receipts.

# Scrutiny of Avast/Jumpshot – Clickstream and Extension Data

- Several browsers (e.g., Chrome, Firefox, Opera) removed consumer-facing cybersecurity extension – Avast – from its browser stores
- News reports speculated cause of removal was that Avast collected too much detailed user data – including clickstream data – that it provided to subsidiary and alt data vendor, Jumpshot
  - Data in the URL might identify the consumer
- Also concerns about lack of transparency/consent and whether this type of data could really be de-identifiable
- Avast responded by requiring entire panel to opt-in
- Jumpshot nonetheless shut down its business

# CCPA

- **Establishes requirements for business regarding:**
- **Transparency:** Provide a privacy policy describing what personal information it collects and CA consumers' rights under CCPA
- **Sale opt out:** Businesses must disclose whether they “sell” consumers' PI and allow the consumer to opt out of such sale
- **Sale Opt in for children:** Businesses must not sell the PI of children under 16 without affirmative consent (from the child if child is 13-16, from parent if child is younger)
- **Access:** Businesses must provide the specific pieces of PI they maintain as well as categories of PI sold/disclosed to third parties
- **Deletion:** Businesses must honor consumers' PI deletion requests (subject to exceptions)
- **Establishes a private right of action related to data breaches**

# CCPA – Definition of Personal Information

**Information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household**

- Broader than GDPR
- Explicitly includes online and device identifiers
- Inferences that can be built based on other PI to build consumer profiles
- Includes information about households

## **Excludes:**

- “Publicly available information” – narrowly defined to include only information derived from public records.
- Aggregate or de-identified information – must implement protections to prevent re-identification of data in order for it to qualify as “deidentified”

# CCPA Impact on Alternative Data

- **Expect to see more de-identified data sets**
  - Neither vendors nor purchasers wish to be bound by CCPA obligations
  - Demand for de-identification will go up
  - Working with raw data will be more challenging
  - Scrutiny about what is truly de-identified may increase
- **Potentially see panels with fewer CA residents/consumers, as either:**
  - California residents are excluded
  - California residents opt out of sales where allowed
- **Diligence process remains important**

# Data Life Cycle



Data  
Collection

Internal  
Use

Products

# Compliance Program Overview

- *Data Collection*
  - *What are you bringing in?*
  - *How is it being collecting?*
- *Internal Use*
  - *What are you doing with the Data?*
  - *How are you protecting it?*
- *Products*
  - *What is the use case for your products?*
  - *How are you protecting them?*

# Data Collection

- *What type of Data is being collected?*
- *Direct Collection vs. Third-Party Collection*
- Internal Processes and Guidelines for Direct Collection
- *Due Diligence Process for Third-Party Collection*

# Due Diligence Process

- *Expert review of Data that is being acquired*
  - *Data Dictionaries*
  - *Business Diligence / Documentation*
- *Chain of Permissioning*
  - *Data Rights*
  - *DDQ*
- *Contractual protections*
  - *Reps and Warranties*
  - *Liability*

# Internal Use & Data Security

- *Establish and implement policy and process to provide guidelines for acquisition, maintenance and use of Data*
- *Align with your Company's purpose for acquiring and using the Data.*
- *Data Security*

# External Use & Productization

- *Risk varies based on the use case your products are intended to serve.*
- *Limitations placed on your customers should align with the intended use case.*
- *Compliance as a Competitive Advantage*

# CONSIDERATIONS FOR USE OF DATA

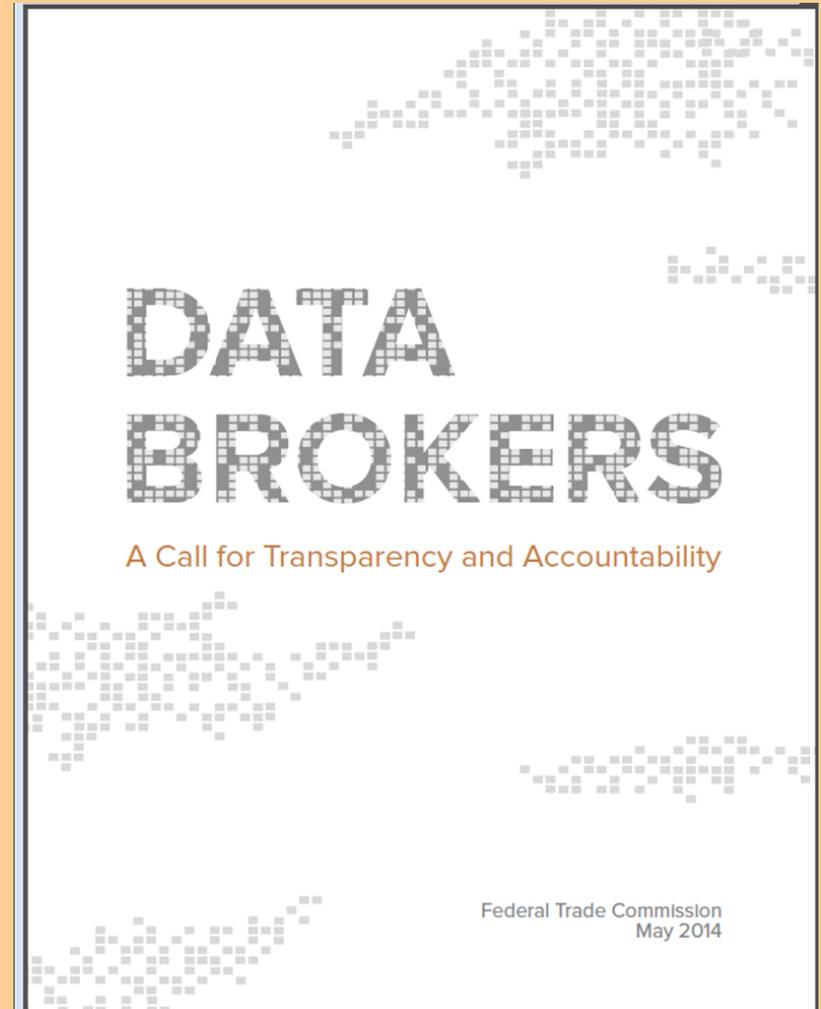
---

# *What is Big Data?*

- The ability to collect consumer data from a variety of sources and use algorithms to:
  - extract hidden information
  - identify correlations
  - make predictions
  - draw inferences
  - glean new insights
- Three Vs:
  - volume,
  - velocity, and
  - variety.

# *Data Broker Report*

- Examined data broker activities, identified some areas of concern, and offered best practices.
- Data brokers acquire info from:
  - Public sources
  - Government
  - Commercial sources
  - Other data brokers



# *Types of Data Acquired*

- Raw Data
  - E.g., name, address, age, ethnicity
- Create Data Elements
  - Derive Inferences from Raw Data
- Create Data Segments
  - Similar characteristics
  - Predict behaviors

# *Types of Products*

- **Marketing:**
  - Direct Marketing
    - Data append
    - Marketing Lists
  - Online Marketing
    - Registration Targeting
    - Collaborative Targeting
    - Onboarding
  - Marketing Analytics
- **Risk Mitigation:**
  - Identity Verification
  - Fraud Detection
- **People Search**

# *Data Broker Report Findings: Characteristics of the Industry*

- Data brokers collect consumer data from numerous sources, largely without consumers' knowledge.
- The data broker industry is complex, with multiple layers of data brokers providing data to each other.
- Data brokers collect and store billions of data elements covering nearly every U.S. consumer.
- Data brokers combine and analyze data about consumers to make inferences about them, including potentially sensitive information.
- 
- Data brokers combine online and offline data to market to consumers online.

# *Data Broker Report Findings: Consumer Choices*

- To the extent data brokers offer consumers choices about their data, the choices are largely invisible and incomplete.
  - Marketing: Limited Access and not all allow correction.
  - Risk Mitigation: Not all provide access and only one allows for correction.
  - People Search Products: Not all allow consumers to opt-out.

# *Data Broker Report Findings: Benefits and Risks*

- Consumers benefit from many of the purposes for which data brokers collect and use data:
  - prevent fraud
  - improve product offerings, and
  - deliver tailored advertisements to consumers.
- Many of the purposes for which data brokers collect and use data pose risks to consumers.
- Storing data about consumers indefinitely may create security risks and lead to liability in the event of a breach.

# Recommendations

- Legislative
  - Notice and disclosure
  - Access and correction
  - Opt out and suppression
- Best Practice
  - Privacy by Design
  - Collect only data needed and establish clear data ownership
  - Dispose of data as it becomes less useful or set a retention period
  - Refrain from collecting from children and teens
  - Ensure downstream users don't use information for FCRA or discriminatory purposes

# *Big Data Report*

- Big Data: A Tool for Inclusion or Exclusion
  - September 2014 Workshop
  - Spring 2014 Seminar on Alternative Scoring Products
- The report:
  - Life cycle
  - Benefits and risks
  - Potentially applicable laws
  - Recent research



# *Life Cycle of Big Data*

- Collection
- Compilation and consolidation
- Data mining and analytics
- Use

# *Benefits*

- Increase educational attainment for individual students.
- Provide access to credit using non-traditional methods.
- Provide healthcare tailored to individual patients' characteristics.
- Provide specialized healthcare to underserved communities.
- Increase equal access to employment.

# *Risks*

- Result in more individuals mistakenly being denied opportunities based on the actions of others.
- Create or reinforce existing disparities.
- Expose sensitive information.
- Assist in the targeting of vulnerable consumers for fraud.
- Create new justifications for exclusion.
- Result in higher-priced goods and services for lower income communities.
- Weaken the effectiveness of consumer choice.

# *Applicable Laws*

- Fair Credit Reporting Act
  - Eligibility determinations
- Equal Credit Opportunity Act
  - Disparate treatment
  - Disparate impact
- Section 5 of FTC Act
  - Deceptive or unfair practices

# *Questions for Legal Compliance*

- If you compile big data for others who will use it for eligibility decisions (such as credit, employment, insurance, housing, government benefits, and the like), are you complying with the accuracy and privacy provisions of the FCRA?
- If you receive big data products from another entity that you will use for eligibility decisions, are you complying with the provisions applicable to users of consumer reports?

# *Questions for Legal Compliance*

- If you are a creditor using big data analytics in a credit transaction, are you complying with the requirement to provide statements of specific reasons for adverse action under ECOA?
- Are you complying with ECOA requirements related to requests for information and record retention?
- If you use big data analytics in a way that might adversely affect people in their ability to obtain credit, housing, or employment:
  - Are you treating people differently based on a prohibited basis, such as race or national origin?
  - Do your policies, practices, or decisions have an adverse effect or impact on a member of a protected class, and if they do, are they justified by a legitimate business need that cannot reasonably be achieved by means that are less disparate in their impact?

# *Questions for Legal Compliance*

- Are you honoring promises you make to consumers and providing consumers material information about your data practices?
- Are you maintaining reasonable security over consumer data?
- Are you undertaking reasonable measures to know the purposes for which your customers are using your data?
  - If you know that your customer will use your big data products to commit fraud or for discriminatory purposes, do not sell your products to that customer. If you have reason to believe that your data will be used for these purposes, ask more specific questions about how your data will be used.

# *Summary of Research Considerations*

- Consider whether your data sets are missing information from particular populations and, if they are, take appropriate steps to address this problem.
- Review your data sets and algorithms to ensure that hidden biases are not having an unintended impact on certain populations.
- Remember that just because big data found a correlation, it does not necessarily mean that the correlation is meaningful. As such, you should balance the risks of using those results, especially where your policies could negatively affect certain populations. It may be worthwhile to have human oversight of data and algorithms when big data tools are used to make important decisions, such as those implicating health, credit, and employment.
- Consider whether fairness and ethical considerations advise against using big data in certain circumstances. Consider further whether you can use big data in ways that advance opportunities for previously underrepresented populations.

# NEW ISSUES

---

# Impact of COVID-19

- Will COVID-19 change the way we think about alternative forms of data collection?
- What safeguards or best practices should we consider as we consider developing new data collection tools (e.g., contact trackers) or taking that information and using it to create insights about the pandemic?

**Questions?**